



THE CLEARING HOUSESM
Advancing Payment Solutions Worldwide

Jeffrey P. Neubert
President and CEO

100 Broad Street
New York, NY 10004
tele 212.612.9203

jeffrey.neubert@theclearinghouse.org

12

October 14, 2003

Public Information Room
Office of the Comptroller of the Currency
250 E Street, S.W.
Mail Stop 1-5
Washington, DC 20219
Attention: Docket No. 03-18

Mr. Robert E. Feldman
Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street, N.W.
Washington, DC 20429
Attention: Comments/OES

Ms. Jennifer J. Johnson
Secretary, Board of Governors
of the Federal Reserve System
20th Street and Constitution Avenue, N.W.
Washington, DC 20551
Attention: Docket NO. OP-1155

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, N.W.
Washington, DC 20552
Attention: No. 2003-35

Re: Proposed Interagency Guidance on Response Programs for
Unauthorized Access to Customer Information and Customer Notice

Ladies and Gentlemen:

The New York Clearing House Association L.L.C.¹ appreciates the opportunity to comment on the proposed Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice – 68 Fed. Reg. 47954-47960 (2003).

¹ The member banks of The Clearing House are: Bank of America, National Association; The Bank of New York; Bank One, National Association; Citibank, N.A.; Deutsche Bank Trust Company Americas; Fleet National Bank; HSBC Bank USA; JPMorgan Chase Bank; LaSalle Bank National Association; Wachovia Bank, National Association; and Wells Fargo Bank, National Association.

The Clearing House supports the Agencies' proposal to provide guidance to financial institutions in developing response programs for unauthorized access to customer information. However, we are concerned that the proposed Guidance may not accommodate the variety of potential security incidents, broad range of financial institutions affected, and rapidly changing legal and technological environment.

We believe that the Agencies' purpose would be better served if the proposed Guidance allowed financial institutions to take into account all relevant circumstances in structuring their response programs. As a result, The Clearing House recommends that the proposed Guidance be revised to permit each financial institution the flexibility to design a response program appropriate for it. Factors that we believe are likely to be relevant include the nature of the financial institution (based on size, complexity, and nature and scope of activities), the type of product or service involved and the form of the security incident.

1. Generally, the Components of the Proposed Response Program Should Permit More Flexibility

The proposed Guidance appears to require a very specific type of response program. Although the program contemplated may be appropriate for some financial institutions or security incidents, we believe that there will be many instances where it may not be.² Given the variety of potential security incidents and the potential impact and burden of notification on both financial institutions and their customers, we believe that additional flexibility would be advantageous.

First, additional flexibility would reflect the broad range of financial institutions that will be affected by the proposed Guidance and would be consistent with the Interagency Guidelines Establishing Standards for Safeguarding Customer Information.³ The Security Guidelines provide that each financial institution must consider which, if any, of the listed security measures are appropriate and, if so, adopt those that are.⁴ In revising the Security Guidelines as part of the comment process, the Agencies have specifically acknowledged that different approaches will be suitable for different institutions.⁵

² As we discuss in detail in Section 2 of this letter, there are several instances where changes to the proposed Guidance could give more flexibility to financial institutions while providing the same, if not better, results for customers.

³ 66 Fed. Reg. 8615-8641 (2001). These guidelines are customarily referred to as the "Security Guidelines".

⁴ Security Guidelines Paragraphs III.C.1.a-h.

⁵ See preamble to the Security Guidelines, pp. 4, 10, 15, 26, 28, 32 and 38.

In addition, financial institutions are accustomed to developing, implementing, enforcing, and competing on the basis of their own response solutions and to the Agencies' supervision of these solutions.⁶ The combination of additional guidance proposed by the Agencies and the additional flexibility that we suggest would enable the continued innovation by financial institutions with respect to customer protection and response programs and further encourage a "race-to-the top" in the adoption and development of new technologies.

Second, we believe that additional flexibility is appropriate in light of the difficulty faced by financial institutions and the Agencies in predicting in advance all of the circumstances that will be relevant in a future security incident. For example, California has recently enacted legislation that requires customer notice if personal information is acquired by an unauthorized person and similar legislation has been introduced in the U.S. Senate.⁷ Both the California Notification Law and the Federal Notification Bill permit delayed customer notification if a law enforcement agency determines that notice will impede a criminal investigation,⁸ but the proposed Guidance does not contemplate this delay. Although the proposed Guidance could be modified to take this particular situation into account, other unexpected or relatively unlikely situations could also warrant a similar result (such as matters of national security).

Third, additional flexibility would take into account that other customer notification requirements could apply. Many financial institutions have customers in multiple states and localities and therefore may be subject to the requirements of multiple jurisdictions. This will be increasingly problematic if additional jurisdictions adopt customer notification legislation. Including additional flexibility in the proposed Guidance would decrease the possibility that a financial institution would be subject to inconsistent standards. This result would be inefficient and potentially could slow the ability of an institution to respond to any particular event.

In light of the preceding, The Clearing House recommends that the Agencies revise the proposed Guidance to adopt the approach of the Security Guidelines: an express statement that financial institutions consider the various components of a response program and

⁶ In the preamble to the Security Guidelines, (1) the Agencies indicated that most institutions already had the expertise to develop, implement and maintain the required information security program, and (2) the Agencies specifically acknowledged that many financial institutions already had in place information security programs that are consistent with the Security Guidelines, the key components of which were derived from security-related supervisory guidance previously issued by the Agencies. See preamble to the Security Guidelines, pp. 4, 25, 29-30 and 38.

⁷ California Senate Bill No. 1386 (2002) became effective on July 1, 2003 (the "*California Notification Law*"). Senator Feinstein introduced the Notification of Risk of Personal Data Act, S. 1350, 108th Cong. (2003), in June 2003 (the "*Federal Notification Bill*").

⁸ See California Notification Law §§ 2 and 4 (codified as Cal. Civ. Code §§ 1798.29(c) and 1798.82(c)), and Federal Notification Bill § 3(a)(4).

implement those components that are appropriate. We believe that this approach is particularly appropriate with respect to the customer notification component.

Ongoing Agency supervision safeguards against the potential that a financial institution will abuse any additional flexibility that is afforded. The Federal Notification Bill explicitly recognizes the benefit of supervision in that it permits supervised financial institutions to develop customer notification procedures that are alternatives to the procedures required of other companies. We believe that the proposed Guidance should take advantage of the opportunity afforded by ongoing supervision and permit financial institutions to continue to be innovators in this area.

2. Specific Revisions

Customer Notice Standard

The Clearing House supports the Agencies' belief that no useful purpose would be served if notices were sent "due to the mere possibility of misuse of some customer information." Significantly, if the threshold for sending customer notices were set too low, the very purpose for establishing a customer notice requirement would be undercut.

The purpose of notifying customers is to alert them to "those situations where enhanced vigilance is necessary to protect against fraud or identity theft." If customers begin receiving notices in the ordinary course and in a variety of circumstances that they believe do not warrant their attention, they may not respond when the potential for misuse is serious. Unless notices are limited or tailored to circumstances that warrant a customer response, there is a substantial risk that they will be perceived as legal technicalities.

Moreover, when customers evaluate whether a security incident truly warrants attention, they will undoubtedly consider all of the facts and circumstances available to them. This will include the nature of the breach, the information accessed, the relevant product, the potential misuse and the financial institution's safeguards. The proposed Guidance does not appear to afford financial institutions with the same flexibility in that it appears to require disclosure unless any level of misuse is unlikely. It therefore may result in more notices than optimal.

We recommend that the Agencies revise the proposed Guidance to recommend disclosure in the case of unauthorized access to sensitive customer information but permit financial institutions to conclude that disclosure is not appropriate, depending on the facts and circumstances. This will allow each financial institution to find its own balance in this area,

taking into account nature and scope of its activities and customers.⁹ As we set forth above, we believe that such flexibility offers little opportunity for abuse.

We also recommend that the proposed Guidance provide that disclosure may be delayed to accommodate a criminal investigation or matter of national security.

Sensitive Customer Information

The Clearing House supports the Agencies' decision to limit the type of information subject to the customer notice standard for the reasons we have described. We suggest that the definition be further refined to exclude account numbers *unless* an account number is acquired in connection with a PIN, access device or other security code (if any) that allows access to a person's account. The combination of a personal identifier and account number is frequently found (such as on any check or deposit slip) and does not raise the concerns contemplated by the proposed Guidance absent the ability to access the account.¹⁰

The Clearing House also suggests that the proposed Guidance clarify that customer notice is required only if sensitive customer information is accessed on the relevant institution's customer information systems.¹¹ To the extent that customer information is provided to a third-party financial institution, company, or governmental authority (either in connection with a transaction, at the request of the customer, or in compliance with law) and subsequently accessed, it would be most appropriate for the third-party to analyze the facts and circumstances and determine whether and/or what type of customer notice is required. In particular, the original financial institution is unlikely to be able to evaluate accurately the steps that have been taken to safeguard the customer's interest in such a circumstance. Failure to clarify this limit could result in customers receiving multiple notices for the same event.

Offer of Assistance

The proposed Guidance requires that financial institutions retain appropriately trained employees to offer assistance to customers if there is a security incident. In addition, the first Key Element of content of a customer notice requires that institutions offer to assist customers to correct and update information on any consumer report relating to the customer.

⁹ Our recommendation also would allow a financial institution to consider the effect of notice on the potential for misuse. For example, a customer notice containing the information required by the proposed Guidance could identify for an intruder the type information that has been accessed.

¹⁰ We do not believe that any additional types of information should be deemed sensitive *prima facie*. We note that the proposed Guidance permits the financial institutions the flexibility to add additional types of information to their response program.

¹¹ As noted in the proposed Guidance, this would include systems maintained by an institution's service providers.

These requirements could impose substantial additional costs on financial institutions. The Clearing House recommends that the Agencies provide financial institutions with the flexibility to tailor any offer of assistance to the circumstance. In particular, The Clearing House believes that any requirement in the Key Elements relating to consumer reports should not go beyond the requirements of the Fair Credit Reporting Act.

Delivery of Customer Notice

As we have noted, we believe that the benefits and burdens associated with the customer notice may differ among financial institutions and events. We therefore recommend generally that the Agencies revise the proposed Guidance to permit financial institutions to tailor the manner in which they notify customers to relevant facts and circumstances. For example, the type of notice that is appropriate may depend on the probability and magnitude of any potential misuse.

We also believe that it would be appropriate for the Agencies to confirm that financial institutions may take into account the cost of delivering notice in determining the appropriate form of customer notice. In particular, we believe that the Agencies should consider specifically permitting less expensive, indirect, notice procedures if either the cost of providing notice or the number of customers to which notice must be provided exceeds a specified threshold. This type of balance would be consistent with the California Notification Law and the Federal Notification Bill and place financial institutions on equal footing with other competitors.

Content of Customer Notice

We recommend that the Agencies revise the required content of any customer notice to be consistent with the general approach discussed in this letter. For example, it will likely not be appropriate in every instance for a customer to remain vigilant for a full two years or to place a fraud alert on the customer's consumer reports.

Securing and Flagging Accounts

The Clearing House agrees with the Agencies that a financial institution should take appropriate measures to contain and control a security incident. We believe, however, that it is in the interest of customers that financial institutions retain the discretion to determine appropriate measures. For example, the proposed Guidance requires that a financial institution secure a customer's accounts until the institution and the customer agree on a course of action. Securing an account can result in substantial inconvenience to customers if it is not warranted. The need for the institution and customer to agree on a course of action may cause delay that further compounds the inconvenience. We respectfully suggest that decisions to implement these measures are appropriately made only in light of the applicable facts at the time.

Notification of Primary Regulator

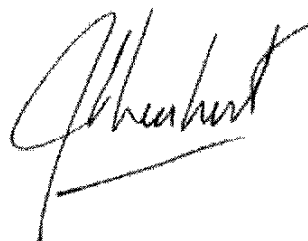
The proposed Guidance appears to require financial institutions to notify their primary Federal regulator of any incident that "could" result in substantial harm or inconvenience to its customers. The use of the word "could" suggests a low threshold for notice, particularly when compared to the proposed customer notice standard (permitting no notice if misuse is reasonably determined to be "unlikely").

The Clearing House does not believe that it is necessary to distinguish security incidents from other activities requiring Suspicious Activity Reports and that the existing SAR regulations and Agency guidance provide an appropriate framework for notification.

* * *

The Clearing House appreciates the opportunity to comment on the proposed Guidance and would be pleased to discuss any of the points raised in this letter in more detail. Should you have any questions, please contact Joseph R. Alexander at (212) 612-9334.

Very truly yours,

A handwritten signature in dark ink, appearing to read "J. Alexander", with a horizontal line drawn underneath the name.